手 続 補 正 書

(法第１１条の規定による補正)

特 許 庁 長 官　殿

１．国際出願の表示　ＰＣＴ／ＪＰ２００４／００３５３３

２．出願人

名　　称　セイコーエプソン　株式会社
SEIKO EPSON CORPORATION

あ て 名　〒163-0811 日本国東京都新宿区西新宿二丁目４番１号
4-1, Nishishinjuku 2-chome, Shinjuku-ku
Tokyo 1630811 Japan

国　　籍　日本国　Japan

住　　所　日本国　Japan

３．代理人

名　　称　特許業務法人湘洋内外特許事務所
The Patent Corporate Body ShowYou International

あ て 名　〒220-0004 日本国神奈川県横浜市西区北幸２丁目９－１０
横浜ＨＳビル　７階
7F, Yokohama HS-Bldg., 9-10, Kitasaiwai 2-chome,
Nishi-ku, Yokohama-shi, Kanagawa 220-0004, Japan

代 表 者　三 品 岩 男　MISHINA Iwao

４．補正の対象　明細書及び請求の範囲

５．補正の内容

（１）　出願時の明細書第１７頁第７行目「軌道」を「起動」に補正する。

（２）　出願時の明細書第１７頁第１４行目「軌道」を「起動」に補正する。

（３）　出願時の請求の範囲第１項第３行目から第4行目「特定のプログラムについての起動指示の検知を行い、特定のプログラムについての起動指示を検知すると、」を、「既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を行うプログラムの最初の起動指示を検知し、前記プログラムの最初の起動指示を検知すると、」と補正する。

（４）　出願時の請求の範囲第２項を削除する。

（５）　出願時の請求の範囲第３項第１行目「請求項２に記載の」を、「請求項１に記載の」と補正する。

（６）　出願時の請求の範囲第４項を削除する。

（７）　出願時の請求の範囲第５項第３行目「特定のプログラムについての」を、「既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を行うプログラムの最初の」と補正する。

（８）　出願時の請求の範囲第５項第３行目「特定のプログラムについての」を、「前記プログラムの最初の」と補正する。

（９）　出願時の請求の範囲第６項を削除する。

（１０）出願時の請求の範囲第７項第２行目と第３行目の間に「既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出する手段と、」を挿入する。

（１１）出願時の請求の範囲第７項第３行目「ネットワークに接続をして通信を実行するプログラムの起動時に、」を、「前記プログラムの起動時の、」と補正する。

（１２）出願時の請求の範囲第９項を削除する。

（１３）出願時の請求の範囲第１０項第１行目から第２行目「請求項７に記載のネットワークセキュリティ強化システムにおいて、」を、「コンピュータのネットワークセキュリティ強化システムにおいて、ネットワークに接続をして通信を実行するプログラムの起動時に、前記ネットワークへの接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備え、」と補正する。

（１４）出願時の請求の範囲第１６項第１行目から第２行目「ネットワークに接続をして通信を実行するプログラムの起動時に、ネットワーク接続処理後他の処理に先行して、」を、「既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出し、前記プログラムの起動時の、ネットワーク接続処理後、他の処理に先行して、」と補正する。

６．添付書類の目録

（１）明細書第１７頁

（２）請求の範囲第１９頁から２２頁

Ｓ２１で、ネットワーク接続中かどうかを判断する。ネットワークに接続中であれば、ステップＳ２２で、接続後に更新したかどうかを判断する。接続後に１回でも更新をした履歴が記録されていれば、ステップＳ２３で、制御プログラムの起動を中止する。もちろん、いったんネットワークを切断してしまった場合には、制御プログラムを起動させる。

次に、本発明の他の実施形態として、ネットワーク制御プログラム１７におけるプログラム自動生成処理１７７により、起動制御プログラムを自動的に生成する例について説明する。このプログラム自動生成処理１７７は、コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、ネットワーク接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、上記通信を実行するプログラムを起動する、起動制御プログラムを自動的に生成するプログラムである。

上記起動制御プログラムの自動生成を実現するには、ネットワーク接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動するという制御プログラムが必要である。しかしながら、コンピュータによって、インストールされている通信用のプログラムが異なる。そこで、あらかじめ、コンピュータにインストールされた、通信用のプログラムを検出し、自動的に起動制御プログラムを生成する手段を設けておく。これにより、各種の通信用プログラムをインストールした任意のコンピュータに対して、上記の機能を容易に付与できる。

図６（ａ）および図６（ｂ）は、ネットワーク接続制御プログラムの別の動作フローチャートである。図６（ａ）は、ネットワーク接続制御プログラム１７をインストールしたときの初期設定動作を示すフローチャートである。

まず、ステップＳ３１で、インストールを完了すると、演算処理装置１００は、ステップＳ３２で、通信用プログラムの検索をする。そして、ステップＳ３３で、通信用プログラムリストを生成する。ここで、そ

請求の範囲

1．（補正後）　ネットワークを介してコンピュータが特定のデータを取得する方法において、

既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を行うプログラムの最初の起動指示を検知し、

前記プログラムの最初の起動指示を検知すると、ネットワークを介して特定のデータを取得するための特定データの取得処理を行い、

その後、前記起動が指示された前記プログラムの起動を行うことを特徴とする、特定のデータを取得する方法。

2．（削除）

3．（補正後）　請求項1に記載の方法において、

前記特定データの取得処理は、セキュリティ対策用ファイルの更新処理である、特定のデータを取得する方法。

4．（削除）

5．（補正後）　ネットワークを介して特定のデータを取得するシステムにおいて、

既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を行うプログラムの最初の起動指示の検知を行う手段と、

前記プログラムの最初の起動指示を検知すると、ネットワークを介して特定のデータを取得するための特定データの取得処理を行う手段と、

特定データの取得処理後、前記起動が指示された特定のプログラムの起動を行う手段と、を備えること
を特徴とする、ネットワークを介して特定のデータを取得するシステム。

6．（削除）

7．（補正後）　コンピュータのネットワークセキュリティ強化システムにおいて、
既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出する手段と、
前記プログラムの起動時の、前記ネットワークへの接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

8．　請求項7に記載のネットワークセキュリティ強化システムにおいて、
セキュリティ対策用ファイルの更新処理を終了後に、当該更新がされたことを報告するメッセージを表示出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

9．（削除）

１０．（補正後）　コンピュータのネットワークセキュリティ強化システムにおいて、

ネットワークに接続をして通信を実行するプログラムの起動時に、前記ネットワークへの接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させる手段を備え、

セキュリティ対策用ファイルの更新処理は、ウィルス対策用の定義ファイルの修正分取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

１１．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

セキュリティ対策用ファイルの更新処理は、パッチファイルの取り込み処理であることを特徴とするネットワークセキュリティ強化システム。

１２．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理を起動させる手段を備えたことを特徴とするネットワークセキュリティ強化システム。

１３．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

ネットワークに接続をして通信を実行するプログラムによる、ネットワーク接続処理後、通信動作の開始前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

１４．　請求項７に記載のネットワークセキュリティ強化システムにおいて、

ブラウザの起動時、画面表示の前に、セキュリティ対策用ファイルの更新処理の起動を要求するメッセージを出力する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

１５．　コンピュータのネットワークセキュリティ強化システムにおいて、

コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

ネットワーク接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、

その後、前記通信を実行するプログラムを起動する、制御プログラムを、自動的に生成する手段を備えたことを特徴とするネットワークセキュリティ強化システム。

１６．（補正後）　既に起動しているコンピュータであって、ネットワークに未接続の状態で、ネットワークに接続をして通信を実行するプログラムの最初の起動時を検出し、

前記プログラムの起動時の、ネットワーク接続処理後、他の処理に先行して、セキュリティ対策用ファイルの更新処理を起動させるように、コンピュータを動作させることを特徴とするネットワークセキュリティ強化プログラム。

１７．　コンピュータにインストールされた、ネットワークに接続をして通信を実行するプログラムを検出し、

前記ネットワークへの接続処理を起動し、セキュリティ対策用ファイルの更新処理を起動し、その後、前記通信を実行するプログラムを起動する制御プログラムを、自動的に生成する処理を、コンピュータに実行させることを特徴とするネットワークセキュリティ強化プログラム。